UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/823,701	03/30/2001	Kenneth W. Aull	15-0225	7427

26294 7590 01/28/2008

TAROLLI, SUNDHEIM, COVELL & TUMMINO L.L.P.
1300 EAST NINTH STREET, SUITE 1700
CLEVEVLAND, OH 44114

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
01/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte KENNETH W. AULL

Appeal 2007-2009
Application 09/823,701
Technology Center 2100

Decided: January 25, 2008

Before JOHN C. MARTIN, ANITA PELLMAN GROSS, and HOWARD B. BLANKENSHIP, *Administrative Patent Judges*.

GROSS, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Aull (Appellant) appeals under 35 U.S.C. § 134 from the Examiner's Final Rejection of claims 1 through 16, which are all of the claims pending in this application. We have jurisdiction under 35 U.S.C. § 6(b).

Appellant's invention relates to a method of preventing ID spoofing in a public key infrastructure. *See generally* Spec. 1. Claims 1 and 5 are illustrative of the claimed invention, and they read as follows:

1. A method of preventing ID spoofing of a public key infrastructure system in an enterprise comprising: allowing a user to access a registration server; upon the registration server receiving identification information from the user and also receiving a request by the user for a new signature certificate, the registration server querying a directory containing reference information of users of the enterprise to obtain information regarding the identified user; and upon the registration server receiving information from the directory indicating that the identified user already possesses a signature certificate, the registration server informing the user that a new signature certificate will not be issued until the old signature certificate has been revoked, thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate and maintaining a one-to-one correspondence between users of the enterprise and signature certificates.

5. A method of preventing ID spoofing of a public key infrastructure system in an enterprise comprising: allowing a user to access a registration server; upon the registration server receiving identification information from the user and also receiving a request by the user for a new signature certificate, the registration server querying a directory containing reference information of users of the enterprise to obtain information regarding the identified user; and upon the registration server receiving information from the directory indicating that the identified user is not in the directory, the registration server informing the user that a signature certificate will not be issued, thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate and maintaining a one-to-one correspondence between users of the enterprise and signature certificates.

The prior art references of record relied upon by the Examiner in rejecting the appealed claims are:

Fisher	US 5,214,702	May 25, 1993
Yacobi	US 5,878,138	Mar. 02, 1999
Vaeth	US 6,308,277 B1	Oct. 23, 2001

Texas Department of Public Safety, "Frequently Asked Questions," pp. 1-4, October 12, 1999, retrieved from the following URL: http://web.archive.org/web/19991012055130/http://txdps.state.tx.us/administration/driver_licensing_control/faq.htm. (Texas DPS)

Tao Zhou, "Directory Integration and the Metadirectory," *Windows ITPro*, July 1999.

Claims 1, 2, 9, and 10 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Yacobi in view of Texas DPS.

Claims 5, 6, 13, and 14 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Yacobi in view of Vaeth.

Claims 3 and 11 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Yacobi in view of Texas DPS and Zhou.

Claims 7 and 15 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Yacobi in view of Vaeth and Zhou.

Claims 4 and 12 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Yacobi in view of Texas DPS and Fisher.

Claims 8 and 16 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Yacobi in view of Vaeth and Fisher.

We refer to the Examiner's Answer (mailed November 8, 2006) and to Appellant's Brief (filed September 27, 2006) and Reply Brief (filed January 1, 2004) for the respective arguments.

SUMMARY OF DECISION

As a consequence of our review, we will affirm the obviousness rejections of claims 1 through 16.

OPINION

Regarding the rejection of claims 1, 2, 9, and 10 over Yacobi in view of Texas DPS, Appellant contends (Br. 11 and 18-19) that the combination

of Yacobi and Texas DPS fails to disclose informing a user that a new certificate will not be issued until the old signature certificate has been revoked. More specifically, Appellant contends that Yacobi does not disclose informing a user at all, and Texas DPS relates to telling a user to surrender a driver's license, not to surrendering signature certificates. Further, Appellant contends (Br. 12-13 and 20-21) that it would not have been obvious to include in Yacobi a step of informing the user that an old certificate must be surrendered before a new one will be issued because Yacobi's process of surrendering old certificates and issuing new ones is automatic. In addition, Appellant contends (Br. 13-17 and 21-24) that Texas DPS is non-analogous art.

The Examiner asserts (Ans. 9) that informing a user that the old signature certificate has been revoked is a "procedural step of 'informing a user' about a procedure [which] is not novel, as evidenced at least by Texas DPS." Further, the Examiner asserts (Ans. 10) that adding a step of informing the user does not change the principle of operation of Yacobi, as "[t]he same operation takes place in Yacobi whether or not a user knows about the existence of a certificate." Furthermore, the Examiner asserts (Ans. 10-11) that users are aware of the existence of certificates, since "Yacobi teaches that if the public key of the user's certificate is believed to have been exposed a user may ask for a new public key with the new certificate he receives." In addition, the Examiner asserts (Ans. 11) that Texas DPS is analogous art as it solves the same problem Appellant solves, "curtail[ing] identification spoofing by requiring surrender of an old form of identification." The issue, therefore, is whether the combination of Yacobi and Texas DPS would have rendered obvious notifying the user that a new

signature certificate will not be issued until the old signature certificate is revoked.

In Yacobi, certification is accomplished by connecting the electronic wallet to the bank's computer, and then the electronic wallet sends a packet including private and public keys along with the user's identification to the bank's computer. Once the user's identity is confirmed, the bank's computer digitally signs the packet and returns a certificate to the electronic wallet. *See* Yacobi, col. 8, l. 62-col. 9, l. 24. The recertification process is similar except that the electronic wallet has to submit the old certificate with the private and public keys. *See* Yacobi, col. 12, ll. 15-22. If the old certificate is on the hot list of bad wallets, the bank "refuses the transaction," which the skilled artisan would expect to include notifying the user that the recertification request has been refused. *See* Yacobi, col. 12, ll. 22-25. Although not specified by Yacobi, the bank would clearly refuse the transaction also if the old certificate were not submitted, which in turn would include notifying the user. Therefore, claims 1, 2, 9, and 10 would have been obvious over Yacobi in view of Texas DPS, with Texas DPS being merely cumulative.

In so holding, we note that Appellant's arguments hinge on the limitation "informing the user that a new signature certificate will not be issued until the old signature certificate has been revoked." The subject matter of the notification is considered non-functional descriptive material, as the content of the message does not affect the claimed method steps. Since Yacobi does notify the user that the transaction has been denied, Yacobi is considered to satisfy the step of informing the user regardless of whether Yacobi informs the user "that a new signature certificate will not be

issued until the old signature certificate has been revoked." Furthermore, assuming for the sake of argument that the recited form of the notification is entitled to weight, it would have been obvious for the notification to include the reason for the refusal and to explain that a new certificate will not be provided until the old certificate has been submitted. Appellant's argument that the users in Yacobi would be unaware of the existence of the certificates (Br. 13) is unconvincing. As noted by the Examiner (Answer 10-11), the users' awareness of the certificates is evident from column 15, lines 19-20: "For non-anonymous systems at expiration, each user gets automatically a new certification, which includes the same old public key with a new expiration (unless the user asks to replace the public key for fear that it has been exposed)." Accordingly, we will sustain the obviousness rejection of claims 1, 2, 9, and 10 over Yacobi in view of Texas DPS.

As to claims 3, 4, 11, and 12, Appellant merely contends (Br. 37-39) that neither Zhou nor Fischer "make[s] up for the aforementioned deficiencies of Yacobi taken in view of Texas DPS" with respect to claims 1 and 9. Since we have sustained the rejection of claims 1 and 9, and Appellant has presented no further arguments regarding Zhou or Fischer, we will likewise sustain the rejections of claims 3 and 11 over Yacobi, Texas DPS, and Zhou and of claims 4 and 12 over Yacobi, Texas DPS, and Fischer.

Appellant contends (Br. 27 and 32) that independent claims 5 and 13 require that the user not possess a signature certificate, but that Yacobi discloses "a user possessing an electronic wallet with a manufacturer-issued certificate, wherein the user is re-certified, and issued another certificate." Therefore, Appellant contends (Br. 27-28 and 33-34) that Yacobi fails to

disclose allowing a user access to a registration server, which receives a request by the user for a new signature certificate. Further, Appellant contends (Br. 28-29 and 34-35) that it would not have been obvious to "include the step of upon a registration server receiving information from a directory indicating that an identified user is not in a directory, the registration server informing the user that a signature certificate will not be issued," because the user would already be in possession of a certificate and, therefore, be in the directory. In addition, Appellant contends (Br. 29-30 and 35-36) that since Vaeth is a less secure system than Yacobi, combining the teachings of Vaeth with those of Yacobi would reduce the security in Yacobi's system.

The Examiner asserts (Ans. 13) that the claims do not preclude the user from having a certificate before requesting one. The Examiner asserts that there are several situations in which a user might already have a certificate, yet the directory would indicate that the user is not in the directory. Further, the Examiner asserts (Ans. 6) that it would have been obvious to combine Vaeth's teaching of informing the user that a certificate will not be issued with Yacobi's system "because notifying a user that a certificate will not be issued informs the user of an authentication error and gives the user the opportunity to take appropriate action." The Examiner also asserts (Ans. 14-15 and 37-38) that there is no security tradeoff by combining Vaeth with Yacobi because Vaeth has a secure process for accessing a certificate request web page. The issues, therefore, are whether it would have been obvious to combine the teachings of Vaeth with Yacobi and whether the combined teachings would suggest the steps of allowing a

user to access a registration server and informing the user that a certificate will not be issued if the user is not in the directory.

Yacobi discloses (col. 4, l. 66-col. 5, l. 13) that the payer (or the user) initially registers with the certifying authority, which can also be the issuer or the bank, and the certificate is later used to verify the identity of the user. Further, when the electronic wallet is issued, it is digitally signed and dedicated to the particular user. Thus, the user accesses a registration server (the certifying authority) to obtain the electronic wallet and a corresponding certificate. Yacobi teaches (col. 8, l. 50-col. 9, l. 24) that the user has to recertify the electronic wallet soon thereafter. The bank's computer (or certifying authority) verifies the initial certificate and then confirms the identity of the user (using the certificate). The recertification process does not involve registering, as the user is already registered.

Yacobi does not disclose the specifics of the original registration process when the user obtains the electronic wallet. However, we can at least infer that the user accesses a registration server (i.e., the bank) which obtains identification information from the user and a request for a new signature certificate. If the user were not to have an account with the bank, then the user would not be in the bank's directory, and an electronic wallet and corresponding certificate would presumably be denied. As to notifying the user that the signature certificate will not be issued, the bank would clearly notify the user that the electronic wallet will not be issued, and, therefore, would indirectly be informing the user that the certificate will not be issued as well. Thus, claims 5 and 13, as well as claims 6 and 14 which

are argued therewith, would have been obvious over Yacobi in view of Vaeth, with the teachings of Vaeth[1] being cumulative.

Regarding claims 7, 8, 15, and 16, Appellant merely contends (Br. 38-39) that neither Zhou nor Fischer "make[s] up for the aforementioned deficiencies of Yacobi taken in view of Vaeth" with respect to claims 5 and 13. Since we have sustained the rejection of claims 5 and 13, and Appellant has presented no further arguments regarding Zhou or Fischer, we will likewise sustain the rejection of claims 7, 8, 15, and 16.

ORDER

The decision of the Examiner rejecting claims 1 through 16 under 35 U.S.C. § 103 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 1.136(a)(1)(iv).

---

[1] Vaeth discloses (col. 7, l. 55-col. 8, l. 54) a requester accessing a certificate request web page and providing identification information, the information being checked against a registration authority database, and the registration authority sending notification of disapproval to the requester if the request is disapproved. Vaeth fails to specify the conditions for disapproval. However, Vaeth implies that if the identification information fails to match the information in the database (or, rather, if the user is not in the database), then the certificate will be disapproved. Thus, Vaeth would appear to at least render obvious independent claims 5 and 13.

AFFIRMED

eld

TAROLLI, SUNDHEIM, COVELL & TUMMINO L.L.P.
1300 EAST NINTH STREET, SUITE 1700
CLEVEVLAND, OH 44114